AMENDMENTS TO THE CLAIMS:

The following listing of claims supersedes all prior versions and listings of claims in this application:

LISTING OF CLAIMS:

1. (Currently Amended) An apparatus comprising:

at least one server configured to send outgoing electronic messages on behalf of terminals connected thereto and to deliver incoming electronic messages to the terminals, each terminal being accessed by one or more users;

the server comprising:

means arranged to generate or receive traffic log data based on at least one traffic characteristic using data derived from the handling of plural electronic messages;

analyzing means arranged to analyze the traffic log data as a function of a predetermined traffic characteristic criterion corresponding to malicious electronic message traffic to identify electronic messages that satisfy the traffic characteristic criterion;

identifying means arranged to identify the destination of the identified electronic messages; and

processing means arranged to send a control message to each of the identified destinations requesting suspension of delivery of the identified electronic messages.

2. (Previously Presented) An apparatus according to claim 1, wherein said server includes:

first means arranged to receive a signal identifying whether or not an identified electronic message is related to an electronic message virus, and

second means arranged to receive data indicative of the success or otherwise of the control message and, in the event that the received signal identifies an electronic message to be a virus and the control message is successful, to trigger deletion of the said identified electronic message.

3. (Previously Presented) An apparatus according to claim 2, wherein:

in the event that a received signal identifies an electronic message to be a virus and the control message is unsuccessful, the second means is arranged to trigger

operation of identifying means and processing means running on a second server corresponding to the destination of the identified electronic message.

4. (Previously Presented) An apparatus according to claim 2, wherein:

in the event that a received signal identifies an electronic message not to be a virus and the control message is successful, the second means is arranged to permit delivery of the identified electronic message.

5. (Previously Presented) An apparatus according to claim 1, wherein said server includes:

first storage for storing data relating to such electronic messages;

further storage for storing a mapping between users and organizational units to which the users belong;

display means for displaying a plurality of images, each representative of an organizational unit;

wherein the server is arranged, in use, such that in response to a request for data relating to a user, the first storage is arranged to output data identifying electronic messages emanating from that user; the further storage is arranged to output data

identifying which of the organizational units that user belongs to; and, for those electronic messages that are identified to satisfy the criterion, the display means is arranged to insert, on the image corresponding to the identified organizational unit, a visual identifier representative of the volume or type of identified electronic messages.

6. (Previously Presented) An apparatus according to claim 5, wherein:

for those electronic messages that are identified to satisfy the criterion, the display means is arranged to display a list of users on an associated image, and for each user on the list, to display details of the volume and/or type of identified electronic messages emanating therefrom.

7. (Previously Presented) An apparatus according to claim 6, wherein:

the display means is arranged to insert a link between the identified organizational unit and the organizational unit corresponding to the identified destination.

8. (Previously Presented) An apparatus for delivering electronic messages, comprising a plurality of apparatus according to claim 1, wherein at least one of the therein servers comprises:

receiving means arranged to receive a request to suspend delivery of an identified electronic message; and

wherein, in response to receipt of a said request, polling means is arranged to check delivery of the identified electronic message, and in the event that it has not been delivered, to block retrieval thereof.

9. (Previously Presented) An apparatus according to claim 8, wherein:

the at least one server includes deleting means for deleting an electronic message; and

in response to receipt of a signal identifying that an identified electronic message is related to an electronic message virus, the deleting means is arranged to check whether retrieval of the identified electronic message has been blocked and, if it has, to delete it.

10. (Previously Presented) An apparatus according to claim 8, wherein:

in the event that the identified electronic message is related to an electronic message virus, and the identified electronic message has not been blocked, the server is arranged to invoke its identifying means and processing means in respect of electronic messages sent by the identified destinations.

11. (Previously Presented) An apparatus according to claim 1, wherein:

the criterion includes at least one of (a) an electronic message type, (b) size of electronic message and (c) number of electronic messages emanating from a user.

12. (Currently Amended) A method of controlling propagation of electronic messages through a network, the network comprising a plurality of servers configured to send outgoing electronic messages on behalf of terminals connected thereto and to deliver incoming electronic messages to the terminals, each terminal being accessed by one or more users, the method comprising:

receiving or generating traffic log data based on at least one traffic characteristic using data derived from the handling of plural electronic messages sent from, or received at, a said server;

analyzing the traffic log data as a function of a specified traffic characteristic criterion corresponding to malicious electronic message traffic to identify those electronic messages that satisfy the criterion;

identifying the destination of the identified electronic messages; and

sending a control message to each of the identified destinations requesting suspension of delivery of the identified electronic messages.

13. (Previously Presented) A method according to claim 12, including:

receiving a signal identifying whether or not an identified electronic message is related to an electronic message virus;

receiving data indicative of the success or otherwise of the control message; and

in the event that the received signal identifies an electronic message to be a virus and the control message is successful, triggering deletion of the said electronic message.

14. (Previously Presented) A method according to claim 13, wherein:

in the event that a received signal identifies an electronic message to be a virus and the control message is unsuccessful, the identifying and sending steps are triggered to be carried out for a server corresponding to the destination of the identified electronic message.

15. (Previously Presented) A method according to claim 13, wherein:

in the event that a received signal identifies an electronic message not to be a virus and the control message is successful, the method includes triggering delivery of the identified electronic message.

16. (Previously Presented) A method according to claim 12, including:

receiving data identifying a mapping between users and organizational units to which the users belong,

displaying a plurality of images, each representative of an organizational unit;

outputting data identifying users who originated the electronic messages that are identified to satisfy the criterion;

identifying, from the mapping, which of the organizational units those users belong to; and

inserting, on an image corresponding to the identified organizational units, visual identifiers representative of the volume or type of identified electronic messages.

17. (Previously Presented) A method according to claim 16, wherein:

for those electronic messages that are identified to satisfy the criterion, the method includes displaying a list of users on an associated image, and for each user on the list, displaying details of the volume and/or type of identified electronic messages emanating therefrom.

18. (Previously Presented) A method according to claim 17, including:

inserting a link between the identified organizational unit and the organizational unit corresponding to the identified destination.

19. (Previously Presented) A method according to claim 1, wherein:

the traffic characteristic criterion includes at least one of (a) type of electronic message, (b) size of electronic message, and (c) number of electronic messages emanating from a user.

20. (Currently Amended) A method of identifying electronic message activity within an organization, the organization having a plurality of users associated therewith, each of which is connected with an organizational unit, the method comprising:

receiving traffic log data defining at least one message traffic characteristic using data derived from the handling of plural electronic messages and emanating from a user relating to electronic messages sent by a user;

analyzing the received traffic log data as a function of a specified traffic characteristic criterion corresponding to malicious electronic message traffic to identify those electronic messages that satisfy the criterion;

receiving data identifying a mapping between users and the organizational units to which the users belong;

displaying a plurality of images, each representative of an organizational unit;

outputting data identifying users who originated the electronic messages that are identified to satisfy the criterion;

identifying, from the mapping, which of the organizational units the users belong to; and

inserting, on an image corresponding to the identified organizational units, visual identifiers representative of the volume or type of identified electronic messages.

21. (Previously Presented) A method according to claim 20, wherein:

the traffic characteristic criterion includes at least one of (a) type of electronic message, (b) size of electronic message, and (c) number of electronic messages emanating from a user.

22. (Previously Presented) Tangible computer-readable storage media containing a computer program, or a suite of computer programs, comprising a set of instructions to cause a computer, or a suite of computers, to perform the method according to claim 12.

23. (Currently Amended) A server configured to send outgoing electronic messages on behalf of terminals connected thereto and to deliver incoming electronic messages to the terminals, each terminal being accessed by one or more users, the server comprising:

message traffic logging means arranged to generate traffic log data based on at least one traffic characteristic using data derived from the handling of plural electronic messages; and

analyzing means to analyze the traffic log data as a function of a specified traffic characteristic criterion corresponding to malicious electronic message traffic to identify those electronic messages that satisfy the criterion.

24. (Previously Presented) A server according to claim 23, the server comprising:

identifying means arranged to identify the destination of said identified electronic messages; and

processing means arranged to send a control message to each of the identified destinations requesting suspension of delivery of the identified electronic messages.

25. (Previously Presented) A server according to claim 1, the server being arranged to receive authentication data from a terminal connected thereto, the authentication data being associated with one or more electronic messages, the server having:

a comparison stage configured to make a comparison between traffic log data corresponding to an identified message and the authentication data corresponding to that message; and

the processing means being arranged to execute a decision to send a suspension request to the identified destination of that message in dependence on the comparison made by the comparison stage.

26. (Previously Presented) A server according to claim 25, wherein:

the authentication data is received in encrypted form, the comparison stage being configured to decrypt the encrypted authentication data and to compare the decrypted data with the traffic log data.

27. (Previously Presented) A terminal for sending and receiving electronic messages to and from a server according to claim 25, wherein the terminal has an interface, the interface having:

a user input for receiving send instructions to send one or more specified electronic messages to a server;

the user input being configured to receive a confirmation input from the user to confirm the send instructions; and

wherein, in response to the confirmation input, the terminal is configured to send the specified electronic messages towards the server and to send authentication data associable with the specified electronic messages.

28. (Previously Presented) A terminal according to claim 27, wherein:

the terminal is configured to detect whether a traffic characteristic criterion relating to the specified electronic message is met, and to request a confirmation input from a user at the user interface in response to the criterion being met.

29. (Previously Presented) A terminal according to claim 27, wherein:

the terminal is configured to transmit the authenticating data in encrypted form.

30. (Currently Amended) A tangible computer-readable storage medium having a computer program stored thereon, the computer program being executable on a terminal to cause the terminal to operate according to the terminal specified in claim 27.

31. (Currently Amended) A tangible computer-readable storage medium having a computer program thereon for sending and receiving electronic messages, the program

being executable on a terminal having a user interface, the computer program being configured to perform the following steps when executed:

(a) invite a user to input at the user interface send instructions for sending one or more electronic messages;

(b) determine if traffic log data based on handling a plurality of electronic messages meets a predetermined traffic characteristic criterion corresponding to malicious electronic message traffic;

(c) if the criterion is met, invite the user to input at the user interface a confirmation input to confirm the send instructions;

(d) upon receipt of the confirmation input, transmit the electronic messages from the terminal; and

(e) transmit authentication data associable with the transmitted electronic message(s).

32. (Previously Presented) A tangible computer-readable storage medium containing a computer program, the computer program being executable on a terminal having electronic messaging software running thereon to reduce the likelihood of a computer virus using the messaging software to propagate from the terminal,

the messaging software being configured to invite the user to input at the user interface send instructions for sending one or more specified electronic messages and, in response to the send instructions, to transmit the messages from the terminal,

said computer program being configured when executed to:

(a) invite a user to input confirmation instructions at the user interface to confirm the send instructions;

(b) only permit the user to send electronic messages once the user has input the confirmation instructions; and

(c) upon receipt of the confirmation instructions, cause the terminal to transmit therefrom authentication data associable with the specified messages.

33. (Previously Presented) A storage medium according to claim 31, wherein:

the authentication data is in encrypted form.

34. (Previously Presented) A storage medium according to claim 31, wherein:

the computer program thereon is configured, when executed, to request a user to input password data as part of the confirmation instructions, and to only permit the terminal to send authentication data once the password data has been input by the user.

35. (Previously Presented) A server according to claim 1, wherein the criterion is met if traffic log data corresponding to a target electronic message indicates that a threshold number of electronic messages and/or a threshold data volume originates from a common terminal or user, in a time interval during which the target electronic message was sent.

36. (Currently Amended) A server configured to send outgoing electronic messages on behalf of terminals connected thereto and to deliver incoming electronic messages to the terminals, each terminal being accessed by one or more users, the server comprising:

receiving means arranged to generate or receive traffic log data based on sending and receipt of plural such electronic messages;

analyzing means arranged to analyze the traffic log data in accordance with a specified traffic characteristic criterion corresponding to malicious electronic message traffic to identify those electronic messages that satisfy the criterion;

identifying means arranged to identify the destination of said identified electronic messages; and

processing means arranged to send a control message to each of the identified destinations requesting suspension of delivery of the identified electronic messages.